POLÍTICA DE CONTROLO DE ACESSOS

PROJETO RGPD

Escola Básica dos 2.º e 3.º Ciclos da Torre (eb23torre)

Câmara de Lobos, 23 de abril de 2026.

Documento Ref.	**P000005**
Versão:	**1**
Data:	**23/04/2026**
Autor:	**Equipa RGPD/Cibesegurança ebtorre**
Proprietário:	**Escola Básica dos 2.º e 3.º Ciclos da Torre**

Revisões - Histórico

Versão	Data	Autor da Revisão	Sumário das Alterações

Distribuição

Nome	Função
Hélder Miranda	Responsável Cibersegurança/Conselho Executivo

Aprovação

Nome	Cargo	Assinatura	Data
Hélder Miranda	Vice-Presidente Conselho Executivo	Assinado por: **HÉLDER JOSÉ VIEIRA MIRANDA** Num. de Identificação: 08154288 Data: 2026.04.29 09:56:32+01'00'	

Índice

0. INTRODUÇÃO

O Controlo de Acessos é parte fundamental da estratégia de Segurança da Informação.

Para protegermos efetivamente a confidencialidade, integridade e disponibilidade dos dados, devemos garantir uma combinação abrangente de controlos físicos e tecnológicos.

O objetivo principal, no que diz respeito ao controlo de acessos, é garantir que sejam adotadas e implementadas medidas de proteção adequadas.

Esta Política deve ser fundamentada num entendimento claro e objetivo dos requisitos associados às atividades exercidas, de forma a garantir o princípio da adequação.

Estes requisitos podem depender de vários fatores, tais como:

- a classificação de segurança da informação armazenada e tratada por determinado serviço ou sistema;
- a legislação relevante que possa ser aplicável;
- as obrigações contratuais com terceiros;
- as ameaças, vulnerabilidades e riscos envolvidos.

Esta Política de Controlo de Acessos é projetada para levar em linha de conta os requisitos da Segurança da Informação e o(s) tipo(s) de informação, estando sujeita a revisões regulares para garantir que a mesma se mantenha apropriada às suas finalidades.

Esta Política aplica-se a todas as pessoas, sistemas, processos e procedimentos que constituem os sistemas de informação da instituição, incluindo, funcionários, fornecedores e terceiros que tenham acesso aos sistemas.

1. REQUISITOS DE CONTROLO DE ACESSOS

Os requisitos do Controlo de Acessos devem ser estabelecidos, de uma forma geral, sempre que sejam incorporados novos serviços ou sistemas e sempre que estes sejam significativamente alterados.

Estes requisitos de Segurança devem adotar alguns princípios gerais, tais como:

- **Defesa por Camadas**: a segurança não deve depender de um único controlo, mas sim, da soma de um determinado número de controlos complementares;
- **Menor Privilégio**: a abordagem padrão deve presumir que o acesso não é necessário, em vez de assumir que é;
- **Acesso Necessário**: o acesso apenas é concedido para as informações necessárias ao desempenho de uma determinada função ou cargo e nada mais;
- **Necessidade de Uso**: os utilizadores apenas devem poder aceder às instalações físicas e tecnológicas necessárias para a sua função ou cargo.

A adesão a estes Princípios Básicos ajudará a manter os sistemas seguros, reduzindo as vulnerabilidades e, consequentemente, o número e a gravidade dos incidentes de segurança que possam vir a ocorrer.

2. GESTÃO DE ACESSOS

Os procedimentos formais de controlo de acessos dos utilizadores devem ser documentados, implementados e atualizados para cada aplicativo e sistema de informação, para garantir o acesso a utilizadores autorizados e impedir os acessos não autorizados.

Os procedimentos devem incluir todo o ciclo de vida do acesso dos utilizadores, desde o registo inicial de novos utilizadores até ao cancelamento do registo, quando o acesso se tornar desnecessário.

Os privilégios de acesso dos utilizadores devem ser revistos regularmente para garantir que apenas são disponibilizados os acessos adequados.

As contas de Administração de Sistemas ou Aplicativos só devem ser fornecidas apenas a utilizadores que sejam indispensáveis para executar as tarefas inerentes à administração do sistema.

Registo de Utilizador e Cancelamento

Qualquer pedido de acesso à rede e aos sistemas da Organização deve ser enviada ao responsável.

Os pedidos devem seguir um procedimento formal que garanta que sejam realizadas verificações de segurança apropriadas e que a conta de acesso só seja criada após autorização.

Cada conta de utilizador terá um nome exclusivo, associado a um indivíduo específico, que não poderá ser compartilhado com nenhum outro utilizador. Não poderão existir contas de utilizador genéricas, nem contas que serão utilizadas por um grupo de pessoas, na medida em que, a adoção deste *modus operandi* não permite cumprir o princípio da responsabilização.

A conta de utilizador deve ser criada com palavras-passe fortes e transmitidas apenas ao Utilizador, através de meios seguros. O Utilizador deve alterar a palavra-passe, assim que efetuar o primeiro acesso ao sistema ou aplicativo.

Sempre que um trabalhador deixar a Organização, os seus acessos aos sistemas e aplicativos devem ser suspensos, no final do último dia de trabalho. É da responsabilidade dos Recursos Humanos solicitar a suspensão dos acessos à Equipa TIC/Cibersegurança.

Em circunstâncias excecionais, sempre que houver a perceção de risco de que o trabalhador possa tomar medidas que possam prejudicar a Organização antes ou após a rescisão contratual, poderá ser aprovada uma suspensão dos acessos, antes de notificada a rescisão.

As contas de utilizador devem ser inicialmente suspensas ou desativadas e não proceder à sua eliminação, antes de decorrido um período de tempo considerado razoável.

Os nomes de contas não devem reutilizados.

Permissões de Acesso

Cada Utilizador apenas deve ter permissões de acesso aos sistemas e dados que sejam compatíveis com a função e tarefas executadas.

Por norma, as permissões de acesso de utilizador devem ser criadas com base na função desempenhada ou a desempenhar, podendo ser criados diversos grupos com diferentes níveis de permissão, os quais serão alocadas a utilizadores específicos.

Não devem ser concedidas permissões a utilizadores que não desempenhem funções para as quais o acesso não seja necessário.

Remoção ou Ajuste de Permissões

Sempre que seja necessário efetuar um ajuste às permissões de acesso dos utilizadores, essas alterações devem ser documentadas e efetuadas de acordo com o processo de alteração de funções dentro da Organização.

Nestas situações, as permissões de acesso devem apenas permitir o acesso a informações necessárias para o desempenho da função, devendo ser removidas permissões referentes à função anterior.

Gestão de Acessos Privilegiados

A gestão de contas com acessos privilegiados, tais como, as contas de administração de sistemas, devem ser identificadas em cada um dos sistemas, aplicativos ou redes e alvo de controlo rigoroso.

Por norma, as contas de administração com acessos privilegiados não devem ser utilizadas no dia-a-dia. Ao invés, devem ser criadas contas específicas que permitam a identificação dos seus utilizadores.

O acesso a contas de administrador apenas deve ser fornecido a indivíduos cujas funções o exijam e que tenham formação suficiente para entender e compreender as implicações da sua utilização.

As contas de utilizadores com acessos privilegiados não devem ser utilizadas em processos com rotinas automatizadas. Quando este tipo de utilização seja indispensável ao bom funcionamento dos sistemas, as palavras-passe devem ser alteradas regularmente.

Autenticação de Utilizadores com conexões externas

De acordo com a Política de Segurança de Rede, o uso de Ponto de Acesso (AP) Wi-Fi não pertencentes à Organização conectados à rede interna pode comprometer seriamente a segurança da rede. Deve ser obtida aprovação antes de se conectar qualquer equipamento à rede da Organização.

Quando for necessário efetuar o acesso remoto à rede, deve-se sempre que possível solicitar a configuração de uma VPN.

Acesso Remoto à Rede por Terceiros

Não devem ser concedidos detalhes de acesso à Rede a terceiros, nomeadamente, fornecedores, subcontratantes ou outros, sem permissão prévia da Equipa TIC/Cibersegurança.

Quando for necessário conceder o acesso a terceiros, este acesso deve ser sempre controlado pela Equipa TIC/Cibersegurança e deve ser interrompido quando o contrato ou a tarefa termine.

Os terceiros com permissões de acesso autorizadas devem contatar previamente a Equipa TIC/Cibersegurança em cada uma das ocasiões que pretendam efetuar uma conexão. Deve-se manter um registo das atividades realizadas pelos terceiros.

Política de Autenticação e Palavra-Passe

Uma palavra-passe forte é uma barreira essencial contra os acessos não autorizados.

Essa área é, frequentemente, identificada como um dos elos fracos na estratégia de segurança de uma Organização.

A Política da EB23Torre é a de usar métodos de autenticação adicionais com base numa avaliação de risco que considere:

- o valor dos ativos protegidos;
- o grau de ameaça que possa existir;
- o custo dos métodos adicionais de autenticação;
- a facilidade de uso dos métodos propostos;
- quaisquer outros métodos relevantes.

A utilização de métodos de autenticação de múltiplos fatores (MFA) deve ser justificada com base nos fatores supracitados, implementados e mantidos de forma segura.

O *Single Sign-On* (Ponto único de entrada) será utilizado dentro da rede interna quando suportado pelos diversos sistemas, a menos que os requisitos de segurança obriguem a um acesso diferenciado.

Se for utilizada a autenticação de um ou mais fatores, a qualidade das palavras-passe dos utilizadores deve ser aplicada em todas as redes e sistemas, de acordo com os seguintes parâmetros:

Parâmetro	Valor
Comprimento mínimo	9
Comprimento máximo	30 ou o limite do sistema em causa
Ciclo de reutilização	Não pode ser o mesmo que qualquer uma das 3 palavras-passe anteriores

Caracteres necessários	letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /)
Semelhança de palavras-passe	A nova palavra-passe não pode utilizar mais do que três caracteres na mesma posição da palavra-passe anterior
Frequência de alteração	Pelo menos a cada 180 dias
Bloqueio da conta	Cinco tentativas de acesso incorreto
Ação de bloqueio	A conta deve ser reativada pelo Administrador de Sistemas
Outros controlos	A palavra-passe não deve conter o nome do utilizador. Não devem também ser usadas palavras-passe consideradas fracas e listadas como palavras-passe mais utilizadas.

Quaisquer exceções a estas regras devem ser previamente autorizadas pela Equipa TIC/Cibersegurança.

Revisão das permissões de acesso

Os administradores de Sistema devem rever, com regularidade, quem tem acesso aos sistemas e quais os respetivos níveis e permissões.

Esta revisão tem por finalidades a identificação:

- de pessoas que não devem ter acessos ativos;
- de contas de utilizador com acesso a informação que não é necessária para a sua função;
- de quaisquer outras situações que não estejam em conformidade com esta Política.

Esta revisão deve ser documentada e quaisquer ações corretivas identificadas e realizadas.

A revisão das contas com acessos privilegiados deve ser efetuada trimestralmente pela Equipa TIC/Cibersegurança para assegurar que esta Política está a ser cumprida.

3. RESPONSABILIDADE DOS UTILIZADORES

Para garantir a segurança da informação e, consequentemente, diminuir o risco e reduzir vulnerabilidades, a EB23Torre aplica diferentes recursos na implementação de controlos eficazes. Não obstante, este esforço será inconsequente, caso os utilizadores não adotem as Políticas de Segurança de Informação com rigor e diligência adequadas, no seu dia-a-dia, ao desempenhar as suas funções.

Muitas violações de segurança são, em grande parte, causadas por acessos não autorizados a contas de utilizadores resultantes de furtos ou adivinhação de palavras-passe por métodos manuais ou automatizados.

É vital que todos os Utilizadores desempenhem a sua parte na proteção dos acessos concedidos e garantam que as suas contas não sejam usadas para prejudicar a Organização.

Para maximizar a segurança da informação, os Utilizadores devem:

- ter uma palavra-passe forte, de acordo com o previsto na presente Política;
- não partilhar a sua palavra-passe;
- não permitir a utilização da sua conta;
- não registar a sua palavra-passe, em papel ou eletronicamente;
- evitar a utilização da mesma palavra-passe para acesso a contas diferentes;
- assegurar-se que qualquer dispositivo que fique desacompanhado, seja bloqueado;
- informar sobre quaisquer alterações das suas funções e requisitos de acesso.

O incumprimento do disposto nesta Política pode levar o Utilizador a incorrer em processo disciplinar, civil ou criminal.